REVERSIBLE ARITHMETIC CODING FOR QUANTUM DATA COMPRESSION

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention generally relates to a method of compressing and decompressing a block of symbols (a block quantum state) emitted by a memoryless quantum Bernoulli source. This presents a simple-to-implement quantum system for projecting, with high probability, the block quantum state onto the typical subspace spanned by the leading eigenstates of the source's density matrix.

Description of the Related Art

Computers and information technology electronically transfer large amounts of data. The data could be stored on a computer disk or in the memory of a computer. The data could be transferred from computer to computer via networks, the internet or over the airways. Today's demands on data transfer range from extremely complex items such as satellite photographs, which require a large amount of memory to simpler items such as e-mail text messages, which demand less memory.

Conventional technology performs the data transfer and storage by reducing the data to an electronic charge or bit which is stored in the computer memory, a CD ROM or disk. The bits are assigned data using a binary code,

which includes only two values, 0 and 1. Thus, each bit may exist as either a 0 or a 1 and a series of bits may be required to represent each piece of data.

The methodology of this approach to data transfer is derived from classical physics. According to these sciences, modern information theory assumes that an information bit can exist in only one of two states, say, 0 or 1. However, classical physics is known to fail spectacularly under many circumstances, for example, when the objects being described are very small or have very large energies. As a result, conventional information theory fails to properly describe how information may be represented and transformed in such physical systems.

Quantum information theory, which is based on the study of quantum mechanics, is capable of more accurately describing and transferring a wider range of data than the conventional binary code method. Similar to the conventional methods, quantum information theory functions by assigning the data to a series of bits, but the bits are called quantum information bits.

In contrast to the classical information bit, a quantum information bit can exist in a superposition of two orthogonal quantum states. Meaning rather than being limited to one of two states, 1 or 0, a quantum information bit can exist in an infinite number of states. A quantum information bit may be any combination of 0 and 1. For example, it can be 40% 1 and 60% 0.

Quantum information can, in principle, provide significant advantages for certain problems. For example, quantum algorithms for calculating discrete logarithms, see, Shor, (P.W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring," in Proceedings of the 35th Annual Symposium on

Foundations of Computer Science, Santa Fe, New Mexico, (Los Alamitos, CA), pp. 124-134, IEEE Computer Society Press, 1994, incorporated herein by reference), and searching unsorted databases, see, Grover, (L.K. Grover, "A fast quantum mechanical algorithm for database search," in Proceedings of the 28th Annual ACM Symposium on Theory of Computation, Philadelphia, Pennsylvania, pp. 212-219, 1996, incorporated herein by reference), have been discovered which are faster than their classical counterparts. Quantum bits, in contrast to classical bits, cannot be copied perfectly, and this is useful in such tasks as quantum cryptography, see, Bennett (C.H. Bennett, G. Brassard, and A.K. Ekert, "Quantum cryptography," Sci. Am., vol. 267, pp. 50-57, Oct. 1992, incorporated herein by reference). Furthermore, Fuchs (C. Fuchs, "Nonorthogonal quantum states maximize classical information capacity," Physical Review Letters, vol. 79, pp. 1162-1165, 1997, incorporated herein by reference), has shown that, rather unexpectedly, there exist certain quantum communication channels for which the optimal classical information transmission rate is achieved only using non-orthogonal quantum states as the symbols. Finally, quite surprisingly, quantum error correction codes have been developed, see, Calderbank et al. (A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, "Quantum error correction via codes over gf (4)," IEEE Trans. Inform. Theory, vol. 44, pp. 1369-1387, July 1998, incorporated herein by reference) and references therein. Such codes might provide the key technology needed to prevent decoherence of quantum states, and, hence, a way to realize large-scale quantum computing devices. For excellent reviews of the field, see, for example, Bennett and Shor

(C.H. Bennett and P.W. Shor, "Quantum information theory," IEEE Trans. Inform. Theory, vol. 44, pp. 2724-2742, October 1998. Commemorative Issue, 1948-1998, incorporated herein by reference), Rieffel and Polak (E. Rieffel and W. Polak, "An introduction to quantum computing for non-physicists," http://xxx.lanl.gov/abs/quant-ph/9809016, 1998, incorporated herein by reference) and Steane (A. Steane, "Quantum computing," Reports on Progress in Physics, vol. 61, pp. 117-173, 1998, incorporated herein by reference).

As our society becomes more modern and more computerized, there is a need to electronically transfer more and more data. To eliminate the limitations of conventional data transfer methods, there is a need for a method of data transfer according to the quantum information theory.

SUMMARY OF THE INVENTION

It is, therefore, an object of the present invention to provide a structure and method for encoding/decoding a block of quantum data including removing trailing eigenstates from the block that have eigenvalues below a predetermined limit to retain leading eigenstates that have eigenvalues above the predetermined limit, and encoding the remaining quantum bits retained in the block. The remaining quantum bits can also include a linear superposition of the leading eigenstates. The predetermined limit is based upon a density matrix of the block. This method of encoding produces encoded quantum bits and can further include decoding the encoded quantum bits by reversing the encoding. The decoding

reproduces the remaining quantum bits and the encoding completely erases the remaining quantum bits. Further, the invention can include outputting only an encoded or decoded result.

The invention may further include a method for block compression of quantum information which may include projecting a block quantum state into a typical subspace having a plurality of eigenstates, encoding the subspace using an encoder, and decoding the subspace using a decoder which generates the block quantum state using a quantum memoryless Bernoulli source. Projecting of the block quantum state into the typical subspace may include analyzing a plurality of eigenvalues contained in a density matrix associated with the block quantum state, determining a plurality of largest eigenvalues, spanning the subspace wherein the eigenstates are associated with the largest eigenvalues to produce a spanned subspace, and projecting the block quantum state into the spanned subspace to produce a project bloack quantum state that lies in a low dimensional typical subspace. The encoder and decoder are quantum-mechanical inverses of each other and the decoding is achieved by performing the encoding in reverse. The encoding can also include using a fixed-rate quantum Shannon-Fano code to compress the projected block quantum state, wherein compression occurs at a per symbol code rate that is slightly higher than a von Neumann entropy limit. Also, the encoding can include creating a representation quantum Shannon-Fano code as a plurality of quantum arithmetic codes and can use the plurality of quantum arithmetic codes to compress the subspace containing the projected block quantum state.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, aspects and advantages will be better understood from the following detailed description of a preferred embodiment of the invention with reference to the drawings, in which:

Figure 1 is a schematic diagram of reversible circuits;

Figure 2 is a flow diagram illustrating a preferred algorithm for encoding data according to the invention;

Figure 3 is a quantum circuit implementing the flow diagram of Figure 2;

Figure 4 is a schematic diagram of a quantum algorithm multiply in which *i* is a classical parameter and B may also be classical, and a schematic circuit symbol for the algorithm;

Figurere 5 is a schematic diagram of a quantum circuit implementing the quantun multiplication algorithm of Figure 4;

Figure 6 is a schematic diagram of algorithms "E" and "D";

Figure 7 is a schematic diagram of a quantum circuit implementing the block encoder algorithm E in Figure 6 and a schematic symbol for the circuit;

Figure 8 is a schematic diagram of a quantum circuit implementing the block decoder algorithm D in Figure 6 and a schematic symbol for the circuit;

Figure 9 is a schematic diagram of a quantum circuit implementing the Shannon-Fano encoder, the corresponding decoder being obtained by running the circuit in reverse; and

Figure 10 is a schematic diagram of a hardware embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

The statistics underlying a quantum memoryless Bernoulli source is completely captured by the source's density matrix. The fundamental idea behind quantum data compression is to analyze the eigen-structure of the joint density matrix associated with a block quantum state emitted by the quantum memoryless Bernoulli source.

The following contributions are discussed in greater detail below. The invention's first contribution is a quantum-mechanical system for projecting the block quantum state onto the subspace spanned by the most important eigenstates of the joint density matrix, that is, the eigenstates corresponding to the largest eigenvalues.

In other words, the invention removes the having eigenstates below a pre-specified minimum. The remaining eigenstates are the most important and are retained. In one embodiment, the invention evaluates the quantum bits by determining whether they are typical. The invention computes, in parallel, an indicator function that is 0 if the eigenstate is typical and 1 otherwise.

The determination of what is typical is made based upon the density matrix. By making a measurement on the quantum bit associated with the

indicator function, with very high probability, the invention projects the block quantum state onto the typical subspace spanned by the leading eigenstates. The invention represents a strengthening of previous results in that the invention holds for fixed block sizes and then delivers a rate of convergence.

The projection onto the typical subspace wipes out the trailing eigenstates, and, hence, the projected quantum state lies in the low-dimensional typical subspace. Thus, the invention reduces the number of different dimensions that must be compressed, making the processing faster and more efficient. Consequently, each leading eigenstate can be represented using roughly the algorithm of the dimension of the typical subspace.

The central problem of quantum data compression is to efficiently compute such low-dimensional representations. The invention also includes a quantum version of the classical Shannon-Fano code to represent and, hence, compress the projected block quantum state using a per symbol code rate that is slightly higher than the von Neumann entropy limit. Conceptually, the invention achieves data compression by dimensionality reduction.

As another contribution, the invention proposes arithmetic codes to efficiently implement quantum Shannon-Fano codes. The invention's arithmetic encoder/decoder uses a certain finite-precision arithmetic process that is inspired by classical arithmetic coding. One point of novelty of the inventive quantum arithmetic coding is the implementation of a finite-precision arithmetic processes in a quantum mechanically reversible fashion. The invention's arithmetic encoder/decoder has a cubic circuit and a cubic computational complexity in the

block size. The proposed encoder and decoder are quantum-mechanical inverses of each other, and constitute a very satisfying example of reversible quantum computation.

The first step of the present invention begins by reviewing the definitions of quantum sources and quantum states relevant to the present coding problem. Further, the invention presents precise quantum counterparts for the classical notions of fidelity and entropy, and describes how encoding and decoding is done using quantum computation.

A classical memoryless Bernoulli source emits a sequence of independent and identically distributed symbols each of which is 0 with probability p or 1 with probability 1 - p, where $0 \leq p \leq 1$. The problem of classical noiseless data compression is the transmitting of sequences of samples emitted by such a source using a minimal number of bits see Shannon, C.E. Shannon, "A mathematical theory of communication," Bell System Technical J., vol. 27, pp. 379-423, 1948, (incorporated herein by reference) which established that on average each symbol can be transmitted in (slightly larger than) $H(p) = - p \log p - (1 - p) \log (1 - p)$ bits with high probability of correct reception, where $H(p)$ is known as the Shannon entropy.

A pure two- dimensional quantum state is known as a quantum bit or qubit. The quantum state of a qubit is mathematically represented by a unit norm vector in a two - dimensional complex vector space (called a Hilbert space) written as H^2. A qubit may be thought of as a column vector, and is usually written using Dirac's ket notation; for example, $|\phi\rangle$ denotes a qubit. The

conjugate transpose of $|\phi\rangle$, namely, $|\phi\rangle^t$, is written in Dirac's braket notation as $\langle\phi|$. The inner product between an ordered pair of qubits, (ϕ,φ), is written in Dirac's braket notation as $\langle\phi|\varphi\rangle$. The invention writes the fidelity between a pair of qubits, (ϕ,φ), as $\langle\phi|\varphi\rangle\langle\varphi|\phi\rangle = |\langle\phi|\varphi\rangle|^2$. Let $|\phi_0\rangle$ and $|\phi_1\rangle$ denote two arbitrary qubits. A quantum memoryless Bernoulli source emits a sequence of independent and identically distributed symbols each of which is $|\phi_0\rangle$ with probability of p or $|\phi_1\rangle$ with probability of 1 - p, where $0 \leq p \leq 1$. The per-symbol distribution of this source is described by the density matrix:

$\rho = p|\phi_0\rangle\langle\phi_0| + (1-p)|\phi_1\rangle\langle\phi_1|$, where $|\phi\rangle\langle\phi|$ denotes the 2 x 2 matrix given by the outer product between the vector $|\phi\rangle$ and its conjugate transpose $\langle\phi|$.

The problem of (pure state) quantum noiseless data compression is the transmitting of such sequences of symbols with high fidelity, using a minimal number of quantum bits. According to Schumacher's theorem, (B. Schumacher, "Quantum coding," Physical Review A, vol. 51, pp. 2738-2747, 1995, [11], incorporated herein by reference), on average each symbol can be transmitted in (slightly larger than) $S(\rho) = -\mathrm{Tr}(\rho \log \rho)$ quantum bits with high probability of correct reception, where $S(\rho)$ is known as the von Neumann entropy. A surprising contrast between the classical and the quantum cases is that

$S(\rho) \leq H(\rho)$, where the equality is achieved if and only if the quantum states $|\phi_0\rangle$ and $|\phi_1\rangle$ are orthogonal. Intuitively, this holds since two non-orthogonal qubits cannot be distinguished with certainty by measurement. The invention will let P and E denote the probability and the expectation, respectively, with respect to the quantum memoryless source.

The invention shall focus on compressing a block of η symbols emitted by the quantum source. Let $|\psi_{[1,\eta]}\rangle \equiv |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots |\psi_\eta\rangle$ be a sequence of symbols emitted by the quantum memoryless source, where $\otimes$ denotes the tensor product, and $|\psi_i\rangle$ represents the *i*th sample from the source, a random state which is either $|\phi_0\rangle$ with probability *p* or $|\phi_1\rangle$ with probability 1 - *p*.

This notation is slightly unconventional. Usually, a quantum state written using the ket notation $|\cdot\rangle$ is definite or pure: it has a von Neumann entropy of zero. However, as shown above, the invention shall find it convenient to use similar notation to denote mixed or random quantum states (random mixtures of pure states); such states will be written with their label in **bold**, in analogy to the often used classical notation for random variables.

Let χ denote a binary string of length η. The invention will let $\chi_{[i,j]}$ denote bits *i* through *j* of X. As an alternative to $\chi_{[1,k]}$, the invention may sometimes write $\chi_{[k]}$ to represent the first k significant bits of X. Similar notation, when used

with qubits, should be clear by analogy. For example, the invention writes $|\psi_{[1,\eta]}\rangle$ as $|\psi_{[\eta]}\rangle$. For every a > 0, the invention writes $0_a = \underbrace{00\cdots0}_{\text{a times}}$ and $1_a = \underbrace{11\cdots1}_{\text{a times}}$. When it is clear how many zeros or ones are necessary, sometimes the subscript will be suppressed.

Although $|\phi_0\rangle$ and $|\phi_1\rangle$ may be non-orthogonal, a basis always exists for H_2 in which the same per-symbol distribution source that emits one of two orthogonal states $|0\rangle$ and $|1\rangle$ with probabilities λ_0 and λ_1 (instead of $\phi_0\rangle$ and $|\phi_1\rangle$ with probabilities p and $1 - p$). The special basis $\{|0\rangle,|1\rangle\}$ is defined as follows. The density matrix ρ characterizes the per-symbol distribution of the original quantum Bernoulli source and is self-adjoint, positive-definite, and has unit trace. Hence, its eigenvalues, say, $\lambda_0 \geq \lambda_1$, are real and nonnegative, and sum to one. If $\lambda_0 \neq \lambda_1$, choose the states $|0\rangle$ and $|1\rangle$ to be eigenvectors of ρ corresponding to λ_0 and λ_1, respectively. By construction, these states are orthonormal, and form a basis for H^2. If $\lambda_0 = \lambda_1$, the select $\{|0,|1\rangle\}$ to be any orthonormal basis of H^2. In this basis, the original symbols $|\phi_0\rangle$ and $|\phi_1\rangle$ are given as $|\phi_0\rangle = \langle 0|\phi_0\rangle|0\rangle + \langle 1|\phi_0\rangle|1\rangle$

$|\phi_1\rangle = \langle 0|\phi_1\rangle|0\rangle + \langle 1|\phi_1\rangle|1\rangle$, and the density matrix can be written as

$\rho = \lambda_0|0\rangle\langle 0| + \lambda_1|1\rangle\langle 1|$, where $\lambda_0 = 1 - \lambda_1 = \rho|\langle 0|\phi_0\rangle|^2 + (1-\rho)|\langle 0|\phi_1\rangle|^2$.

Furthermore, the invention can now write $S(\rho) = H(\lambda_0)$.

For $1 \le i \le n$, the mixed quantum state $|\psi_i\rangle$ can be written as

$$|\psi_i\rangle = \langle 0|\psi_i\rangle|0\rangle + \langle 1|\psi_i\rangle|1\rangle,$$

where $\langle 0|\psi_i\rangle$ and $\langle 1|\psi_i\rangle$ are random quantities such that

$$E\,|\langle 0|\psi_i\rangle|^2 = \lambda_0 \text{ and } E|\langle 1|\psi_i\rangle|^2 = \lambda_1. \tag{2}$$

The sequence of symbols $|\psi_{[\eta]}\rangle$ in Eq. (1) is a mixed quantum state in the Hilbert space $H_2^{\otimes\eta} = \otimes_{i=1}^{\eta} H2$. Using properties of the tensor product, the foregoing can be written as

$$\begin{aligned} |\psi_{[\eta]}\rangle &= \otimes_{i=1}^{\eta}|\psi_i\rangle \\ &= \otimes_{i=1}^{\eta}\sum_{X_i=0}^{1}\langle X_i|\psi_i\rangle|X_i\rangle \\ &= \sum_{X\in\{0,1\}^{\eta}}\langle X|\psi_{[\eta]}\rangle|X\rangle, \end{aligned} \tag{3}$$

where

$$|X\rangle = \otimes_{i=1}^{\eta}|X_i\rangle \text{ and } \langle X|\psi_{[\eta]} = \prod_{i=1}^{\eta}\langle X_i|\psi_i\rangle.$$

Now,

$$E|\langle X|\psi_{[\eta]}\rangle|^2 \overset{(a)}{=} \prod_{i=1}^{\eta} E|\langle X_i|\psi_i\rangle|^2 \overset{(b)}{=} \prod_{i=1}^{\eta}\lambda_0^{(1-X_i)}\lambda_1^{X_i} \equiv \Lambda(X;\lambda_0,\lambda_1), \tag{4}$$

where (a) follows from independence and (b) follows from Eq. (2). The $2n$ quantum states $|X\rangle$, $X \in \{0, 1\}^n$, can be thought of as the eigenstates of the tensor

product density matrix $\rho^{\otimes n} = \otimes_{i=1}^{\eta} \rho$, and the numbers $\Lambda(X;\lambda_0,\lambda_1)$ as the corresponding eigenvalues. Note that the eigenstates $|X\rangle$, $X \in \{0,1\}^n$ constitute an orthonormal basis for the Hilbert space $H_2^{\otimes \eta}$.

It follows from Eq. (3) that the invention writes the message $|\psi_{[n]}\rangle$ to be encoded as a linear superposition of the 2^n eigenstates (e.g., $|X\rangle$, $X \in \{0, 1\}^n$). The "randomness" of the message is completely contained in the coefficients $\langle X|\psi_{[n]}\rangle$, and the eigenstates are not a function of the particular message to be transmitted. Physically, the randomness is embedded entirely in the complex amplitude associated with each path or eigenstate.

The encoding and decoding of classical information is specified by a mapping between bit-strings. Similarly, for quantum information, the invention specifies a mapping between quantum states. However, additional reversibility constraints must be satisfied with quantum states. For example, a reversible transformation must conserve energy. Since quantum states are mathematically represented by vectors with unit norm, reversible transformations must preserve the norm. It also turns out that with the appropriate description of the system, the most general transformation preserves orthogonality between states. If the quantum states in H_2^n as 2^n- dimensional column vectors, then most general transformations are described by 2^n x 2^n unitary matrices acting on the Hilbert space of the quantum states. Again, a unitary matrix is one whose conjugate transpose is its inverse.

This model of computation subsumes classical computation, because mappings between bit-strings can be described as permutation matrices acting on the basis elements of the Hilbert space. Unitary transforms are always invertible or reversible. All irreversible (classical) computation can be made reversible with only a polynomial amount of overhead (see C. H. Bennett, "Logical reversibility of computation," IBM J. Res. Dev., vol. 17, pp. 525-532, 1973, incorporated herein by reference). However, not all unitary transforms represent reversible classical computation. Not all unitary transforms can be described by permutation matrices. A unitary transform can be completely specified by its action on all the basis elements of a Hilbert space. Transformations which are not permutations take basis elements to superpositions of basis elements; these are at the heart of the speedup of quantum computation and quantum error correction.

Quantum algorithms are generally very difficult to construct, but choosing the eigenstates $|X\rangle$, $X \in \{0,1\}^n$, as the basis vastly simplifies the descriptions of the inventions encoding and decoding transforms. In this special basis, the invention only employs unitary transformations which are permutations of basis elements to achieve the inventions goal. These transforms shall be applied to input states which are generally in non-classical superpositions of basis elements. As suggested by Deutsch, (D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer," Proc. R. Soc. Land. A, col. 400, pp. 97-117, 1985, incorporated herein by reference), it is convenient to think of what happens as being "quantum parallelism". For an input $|\phi\rangle = a|0\rangle+b|1\rangle$, a computation U produces $U|\phi\rangle = aU|0\rangle+bU|1\rangle$, by linearity. For example, two

"classical" computation happen in parallel, one with input $|0\rangle$ and the other with, $|1\rangle$, with the two computational paths being weighted with complex amplitudes *a* and b, respectively. Similar observations hold for arbitrarily large states. As long as U is simply a permutation, these different paths never interfere and a coherent quantum state is maintained.

The invention symbolically describes encoding and decoding unitary transforms for quantum information using algorithms which at first glance look very classical, but in reality, are specially constructed to be quantum. Three characteristics make the invention's algorithms quantum-mechanical. First, they are reversible, which is required as previously explained. Second, they completely erase their inputs, which is a necessity because quantum states cannot be cloned (see W. K Wootters and W.H. Zurek, "A single quantum cannot be cloned," Nature, vol. 299, pp. 802-3, 1982, incorporated herein by reference) and D. Dieks, "Communication by EPR devices," Physics Letters A vol. 92 (6), pp. 271-272, 1982, incorporated herein by reference), and thus there is no sense to a sender sending a faithfully encoded quantum state elsewhere without erasing their own knowledge of that state in the process. Third, the invention produces no information other than the encoded (or decoded) state, which allows differentiation between computational paths. Producing such entanglement would ruin the superposition which is being encoded, because any potential for obtaining "which path" information implies the existence of a physical measurement which would (at least partially) collapse the superposition state. Fundamentally, this non-

disturbance requirement is deeply related to the no-cloning theorem, and it is a subtle, but very important point.

The invention employs for clarity of exposition, quantum circuits, which succinctly capture the same information as the algorithms, and often effectively convey additional structural information about the procedure. A wide body of knowledge about quantum circuits exists (see, A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVicenzo, N. Margolus, P.W. Shor, T. Sleator, J. Smolin, and H. Weinfurther, "Elementary gates for quantum computation," Physical Review A, vol. 52, no. 5, pp. 3457-3467, 1995, incorporated herein by reference, and A. Barenco, "A universal two-bit gate for quantum computation," Proc. R. Soc. London A. Vol. 449, no. 1937, pp. 679-683, 1995, incorporated herein by reference), but only the subset shall be drawn from it, which is convenient for describing reversible classical circuits, including the controlled-NOT and swap gates, as shown in Figure 1.

Figure 1 illustrates two quantum gates which are used in later quantum circuits. The first gate is the controlled-NOT gate, which produces x' = x and y' = x $\oplus$ y ($\oplus$ denoting (bitwise) addition module 2). The second gate is the swap gate, for which x' = y and y' = x. Time goes from left to right. A final useful notation for expressing the coding procedure is that, given a fractional number (e.g., ζ,$0 \leq \zeta \leq 1$), let $\zeta = 0.\zeta_1 \zeta_2 \zeta_3 \cdots$, denote a binary representation of the number. This number can be associated to a pure quantum state $|\zeta\rangle = |\zeta_1\rangle \otimes |\zeta_2\rangle \otimes |\zeta_3\rangle \otimes \cdots$ in the infinite-dimensional Hilbert space H_2^{∞}. This allows for representation of a fractional real number as a quantum state.

As shown in Figure 2, a symbolic system or "psuedocode" for computing Eq. (6), discussed below. "$\leftarrow$" denotes an assignment operation. When describing a pre-existing state or comparison operation, the invention uses "=". A temporary quantum register $|w\rangle$ of length [log n] is used. This register is initialized and finalized to $|0^{\lceil \log n \rceil}\rangle$. The precise value of τ should satisfy Eq. (8), below and will be specified further below in Eq. (16).

Figure 3 illustrates a quantum circuit implementing the system in Figure 2. The gates labeled as U_+ and U_- implement lines 2-4 and lines 10-12 of the system, respectively. These gates are quantum-mechanical inverses of each other. The gate $U_{\geq}$ implements lines 6-8 of the system. As in "Barenco", supra, the invention generally uses rounded symbols to denote the control qubits, and boxed symbols to indicate the targets, with the exception of "$\otimes$" which always sits on a target. The $/^{\lceil \log n \rceil}$ notation indicates a wire bundle with $\lceil \log n \rceil$ qubits. This is proven in the adaption of the technique in Hoeffding (W. Hoeffding, "Probability inequalities for sums of bounded random variables," American Statistical Association Journal, vol. 58, pp. 13-30, 1963, incorporated herein by reference).

The basic idea of quantum data compression is that the eigenstates associated with smaller eigenvalues can be discarded without incurring significant loss of average fidelity. This goal will be attained by employing a measurement of a certain quantum observable associated with the given message, described further below.

Let $w(X)$, $X \in \{0,1\}^n$, denote the Hamming weight of the string X, for example, the number of ones in the string. It follows from Eq. (4) that it can be written

$$\Lambda(X;\lambda_0,\lambda_1) = \lambda_0^{n-w(X)} \lambda_1^{w(X)} \tag{5}$$

Since $\lambda_0 \geq \lambda_1$, it follows from Eq. (5) that smaller the Hamming weight of an eigenstates the larger the eigenvalue associated with the eigenstate. Let $\tau \geq 0$ denote a truncation threshold. Let G_τ and B_τ denote the sets of "good" and "bad" eigenstates such that

$$G_\tau = \{X | w(X) < \tau\}$$
$$B_\tau = \{X | w(X) \geq \tau\}.$$

With appropriate values of τ, the subspace spanned by the good eigenstates, namely,

$$\text{span}\{|X\rangle | X \in G_\tau\}$$

becomes the typical subspace that contains most of the information present in an average quantum message.

For every eigenstate $|X\rangle$, $X \in \{0,1\}^n$, let $I_\tau(X)$ denote the good-bad indicator function such that

$$I_\tau(X) = \begin{cases} 0 \text{ if } X \in G_\tau, \\ 1 \text{ if } X \in B_\tau. \end{cases}$$

The following transformation is now computed:

$$|X,0\rangle \rightarrow |X,I_\tau(X)\rangle. \tag{6}$$

The invention exhibits a quantum system for computing Eq. (6) in Figure 2, which is implemented by the quantum circuit in Figure 3. This system makes use of subroutines previously described in the literature (see R. Cleve and D.P. DiVicenzo, "Schumacher's quantum data compression as a quantum computation," Physical Review A, vol. 54, pp. 2636-2650, October 1996, incorporated herein by reference) for conditional addition and subtraction, and comparison. Using Eq. (3), the action of the system on the quantum message can be written as

$$|\psi_{[\eta]},0\rangle \rightarrow \sum_{X\in\{0,1\}^{\eta}} \langle X|\psi_{[\eta]}\rangle |X, I_{\tau}(X)\rangle \equiv |\hat{\psi}_{[\eta]}, I_{\tau}\rangle, \tag{7}$$

where $|\hat{\psi}_{[\eta]}, I_{\tau}\rangle$ is an output state in which I_{τ} is now a function of $\hat{\psi}_{[\eta]}$ and thus, in general, is entangled with it. Let

$$\{|I_{\tau}\rangle \overset{m}{=} |0\rangle\} \text{ or } \{|I_{\tau}\rangle \overset{m}{=} |1\rangle\}$$

denote the two possible events corresponding to measuring $|I_{\tau}\rangle$ to be $|0\rangle$ or $|1\rangle$, respectively. The truncation threshold τ is determined to ensure that the probability of the event $\{|I_{\tau}\rangle \overset{m}{=} |0\rangle\}$ is close to 1.

Assuming that $\frac{1}{2} < \lambda_0 < 1$, for a fixed $n \geq 1$ and a fixed $\delta > 0$, it is set that

$$\tau \geq \left\lceil \eta\left(\lambda_1 + \frac{\delta}{\log \lambda_0 / \lambda_1}\right)\right\rceil, \tag{8}$$

then

$$P\{|I_{\tau}\rangle \overset{m}{=} |0\rangle\} = 1 - P\{|I_{\tau}\rangle \overset{m}{=} |1\rangle\} \geq 1 - 2^{\frac{2n\delta^2}{(\log \lambda_0 / \lambda_1)^2}}. \tag{9}$$

The invention adapts the technique in Hoeffding (29, W. Hoeffding, "Probability inequalities for sums of bounded random variables," *American Statistical Association Journal*, vol. 58, pp.13-30, 1963.) incorporated herein by reference:

$$P\left\{\left|I_\tau \overset{m}{=} |1\rangle\right\}\right\} = \sum_{\chi \in B\tau} E\left|\left\langle \chi \middle| \psi_{[\eta]} \right\rangle\right|^2$$

$$\overset{(a)}{=} \sum_{\chi \in B\tau} \Lambda\left(\chi; \lambda_0, \lambda_1\right)$$

(b)

$$\leq \sum_{\{X \mid -\log \Lambda(X;\lambda_0,\lambda_1) \geq \eta(S(\rho)+\delta)\}} \Lambda(X,\lambda_0,\lambda_1)$$

(c)

$$\leq \min_{\gamma > 0} \left[\sum_{\left\{X \mid -\log \Lambda(X;\lambda_0,\lambda_1) \geq \eta(S(\rho)+\delta)\right\}} 2^{\gamma\left(-\log \Lambda(X;\lambda_0,\lambda_1) - \eta(S(\rho)+\delta)\right)} \Lambda\left(\chi; \lambda_0, \lambda_1\right) \right]$$

$\leq \min$

$$\gamma > 0 \left[2^{-\gamma\eta\delta} \sum_{\chi \in \{0,1\}^{\eta}} 2^{\gamma\left(-\log\Lambda(\chi;\lambda_0,\lambda_1)-\eta S(\rho)\right)\Lambda(\chi;\lambda_0,\lambda_1)} \right]$$

$$= \min_{\gamma>0} \left[2^{-\gamma\eta\delta} \prod_{i=1}^{\eta} \left(\lambda_0 2^{\gamma\left(-\log\lambda_0 - S(\rho)\right)} + \lambda_1 2^{\gamma\left(-\log\lambda_1 - S(\rho)\right)} \right) \right]$$

(d)

$\leq \min$

$$\gamma > 0 \left[2^{-\gamma\eta\delta} \prod_{i=1}^{\eta} \left(2^{(1/8)\gamma^2\left(\log(\lambda_0/\lambda_1)\right)^2} \right) \right]$$

(e) $2^{-2\eta\delta^2/\left(\log(\lambda_0/\lambda_1)\right)^2}$

where (a) follows from Eq. (4); (b) follows since $\lambda_1^{\theta}\lambda_0^{\eta-\theta}, 0 \leq \theta \leq \eta$ is a decreasing function of 0, and, hence, by using Eq. (8)

$$\lambda_1^{\tau}\lambda_0^{\eta-\tau} \leq \lambda_1^{\eta\lambda_1+\eta\delta/\left(\log(\lambda_0/\lambda_1)\right)}\lambda_0^{\eta-\eta\lambda_1-\eta\delta/\left(\log(\lambda_0/\lambda_1)\right)}$$

$$= \lambda_1^{\eta\lambda_1} \lambda_0^{\eta\lambda 0} \left(\frac{\lambda_1}{\lambda_0}\right)^{\eta\delta/(\log(\lambda_0/\lambda_1))}$$

$$= 2^{-\eta(s(\rho)+\delta)} .$$

(c) holds for all $Y > 0$, since

$$2^{r\left(-\log\Lambda(x,\lambda_0,\lambda_1)-\eta(s(\rho)+\delta)\right)} \geq 1;$$

(d) follows from [W. Hoeffding, "Probability inequalities for sums of bounded random variables," *American Statistical Association Journal*, vol. 58, pp. 13-30, 1963, incorporated herein by reference, (4.16)], if $1/2 < \lambda_0 < 1$; and (e) follows by selecting the minimizing value

$$\gamma = \frac{4\delta}{\left(\log(\lambda_0 / \lambda_1)\right)^{2.}}$$

Observe that $\left|\hat{\psi}_{[\eta]}\right\rangle$ and $\left|I_\tau\right\rangle$ in Eq. (7) are, in general, entangled. Hence, a measurement on the last qubit will irreversibly effect the first n qubits. Precisely,

using yon Neumann's postulate (J. Von Neumann, *Mathematical Foundations of Quantum Mechanics*. Princeton, USA: Princeton University Press, 1955. Chapter VI), incorporated herein by reference, the effect on $|\hat{\psi}_{[\eta]}\rangle$ of measuring $|I_\tau\rangle$ is the following:

$$|\hat{\psi}_{[\eta]}\rangle = \begin{cases} \dfrac{1}{\sqrt{\sum_{\chi \in G_\tau} |\langle \chi | \psi_{[\eta]} \rangle|^2}} \sum_{\chi \in G_\tau} \langle \chi | \psi_{[\eta]} \rangle | \chi \rangle \text{ if } \{|0\rangle\} \\ \dfrac{1}{\sqrt{\sum_{\chi \in B_\tau} |\langle \chi | \psi_{[\eta]} \rangle|^2}} \sum_{\chi \in B_\tau} \langle \chi | \psi_{[\eta]} \rangle | \chi \rangle \text{ if } \{|I_\tau\rangle \overset{m}{=} |1\rangle\}. \end{cases}$$

In other words, if the event $\{|I_\tau\rangle \overset{m}{=} |0\rangle\}$ occurs, then $|\hat{\psi}_{[\eta]}\rangle$ will collapse to the renormalized projection of the message $|\psi_{[\eta]}\rangle$ onto the subspace spanned by the good eigenstates, otherwise $|\hat{\psi}_{[\eta]}\rangle$ will collapse to the renormalized projection of the message $|\psi_{[\eta]}\rangle$ onto the subspace spanned by the bad eigenstates. Thus, with high probability, the bad eigenstates are discarded.

It follows from Theorem 3.1 that the event $\{|I_\tau\rangle \overset{m}{=} |0\rangle\}$ occurs with very high probability. When this event occurs, the invention now illustrates that, the collapsed state $|\hat{\psi}_{[\eta]}\rangle$ is not much different from the original message $|\psi_{[\eta]}\rangle$, that is, the average fidelity between the two is close to the maximum possible

value of l. Recall that the average fidelity is the probability that the message $\left|\hat{\psi}_{[\eta]}\right\rangle$ passes a test for being the same as the original message $\left|\psi_{[\eta]}\right\rangle$, whence the test is conducted by someone who knows the original message, see, Schumacher (11, B. Schumacher, "Quantum coding," *Physical Review A*, vol. 51, pp. 2738-2747, 1995.) incorporated herein by reference.

If the previous hypotheses holds, then

$$E\left[\left|\langle\psi_{[\eta]}\left|\hat{\psi}_{[\eta]}\right\rangle\right|^2\left|\left\{\left|I_\tau\right\rangle\stackrel{m}{=}\left|0\right\rangle\right\}\right.\right] \geq 1-2^{-\left(\log\lambda_0/\lambda_1\right)^2}.$$

This is shown in the following.

$$E\left[\left|\langle\psi_{[\eta]}\left|\hat{\psi}_{[\eta]}\right\rangle\right|^2\left|\{I_\tau\rangle\stackrel{m}{=}\left|0\right\rangle\}\right.\right]$$

$$= E\left[\left|\sum_{\chi\in\{0,1\}^\eta}\sum_{\xi\in\{0,1\}^\eta}\left\langle\chi\left|\psi_{[\eta]}\right\rangle^t\langle\xi\left|\hat{\psi}_{[\eta]}\right\rangle\langle\chi\right|\xi\right|^2\left|\left\{\left|I_\tau\right\rangle\stackrel{m}{=}\left|0\right\rangle\right\}\right.\right]$$

$$\underline{\underline{(a)}}\ E\left[\left|\sum_{\chi\in\{0,1\}^\eta}\langle\chi\left|\psi_{[\eta]}\right\rangle^t\langle\chi\left|\hat{\psi}_{[\eta]}\right\rangle\right|^2\left|\left\{\left|I_\tau\right\rangle\stackrel{m}{=}\left|0\right\rangle\right\}\right.\right]$$

$$\underline{\underline{(b)}}\ \mathrm{E}\left|\frac{\sum_{\chi\in G\tau}\left|\langle\chi|\psi_{[\eta]}\rangle\right|^2}{\sqrt{\sum_{\chi\in G\tau}\left|\langle\chi|\psi_{[\eta]}\rangle\right|^2}}\right|^2$$

$$= \mathrm{E}\sum_{\chi\in G\tau}\left|\langle\chi|\psi_{[\eta]}\rangle\right|^2$$

$$\underline{\underline{(c)}}\ \sum_{\chi\in G\tau}\Lambda\left(\chi;\lambda_0,\lambda_1\right)$$

$$\underline{\underline{(d)}}\ 1-\sum_{\chi\in B\tau}\Lambda\left(\chi;\lambda_0,\lambda_1\right)$$

$$\overset{(e)}{\geq}\ 1-2^{-\frac{2\eta\delta^2}{(\log\lambda_0/\lambda_1)^2}}$$

where (a) follows by using the orthonormality of the eigenstates; (b) follows from Eq. (10); (c) follows from Eq. (4); (d) follows by applying the binomial theorem to $1=\left(\lambda_0+\lambda_1\right)^{\eta}$; and (e) follows from the foregoing.

The foregoing, represents a strengthening of Schumacher's pioneering result in that they hold for fixed block sizes and they deliver a rate of convergence.

The invention proposes the following scheme for transmitting the quantum message $\psi_{[n]}$.

compute Eq. (7)

measure $|I_\tau\rangle$

if $\left(\left\{|I_\tau\rangle \stackrel{m}{=} |0\rangle\right\}\right)$ then

transmit $|\hat{\psi}_{[\eta]}\rangle$

else

do nothing

It follows that the above scheme has high average fidelity with high probability, and only an exponentially small probability of failing to transmit any information. This can be explained as follows: the desirable event $\left(\left\{|I_\tau\rangle \stackrel{m}{=} |0\rangle\right\}\right)$ occurs with probability close to 1. And, in the case of this even, only the bad eigenstates are discarded.

From now on, it is assumed that the event $\left\{|I_\tau\rangle \stackrel{m}{=} |0\rangle\right\}$ has occurred, and the following focuses on transmitting $|\hat{\psi}_{[\eta]}\rangle$. It follows from Eq. (10) that $|\hat{\psi}_{[\eta]}\rangle$ lies in the typical subspace spanned by the good eigenstates. The invention selects the truncation threshold such that the typical subspace has dimension at most $2^{\eta(S(\rho)+\delta)+1}$ which is much less than the original dimension of 2η. Hence, by appropriately "relabeling" the leading eigenstates, the invention should be able to represent, and, hence, compress the n qubit message $|\hat{\psi}_{[\eta]}\rangle$ to $\eta\left(S(\rho)+\delta\right)+1$

qubits. The main problem, which is now tackled, is how to compute such a dimensionality reducing or relabeling transformation efficiently.

The eigenvalues λ_0 and λ_1 are real numbers, and, when represented as fractional binary numbers, may require an infinite precision to represent. Since, in practice, the invention can only store and manipulate a finite number of bits, from now on, the invention approximates the eigenvalues using fractional numbers with q significant bits after the binary point. In particular, the invention lets $\hat{\lambda}_0$ denote the fractional number obtained by truncating all but the q most significant bits of λ_0. And, the invention lets $\hat{\lambda}_1 = \lambda_1 + \left(\lambda_0 - \hat{\lambda}_0\right)$.

Since, $\lambda_0 + \lambda_1 = 1$, it follows that $\hat{\lambda}_1$ has at most q nonzero significant bits, and the remaining bits must be zeroes. Furthermore,

$$\hat{\lambda}_0 + \hat{\lambda}_1 = 1.$$

In the rest of the disclosure, instead of the original eigenvalues, the invention will use $\hat{\lambda}_0$ and $\hat{\lambda}_1$. To be sure, such an approximation will slightly increase the per symbol rate needed for compression by

$$D\left(\lambda_0 \middle\| \hat{\lambda}_0\right) = \lambda_0 \log\left(\lambda_0 / \hat{\lambda}_0\right) + \lambda_1 \log\left(\lambda_1 / \hat{\lambda}_1\right).$$

The quantity $D(\bullet\|\bullet)$is known as the relative entropy or as the Kullback-Leibler distance. This increase in the per-symbol rate can be made as small as desired by selecting a large enough q. However, the invention will subsequently demonstrate that the amount of quantum hardware required to implement the encoders and decoders will increase quadratically in q.

The invention now introduces a quantum "encoder' transformation that transforms each eigenstate $|\chi\rangle, \chi \in \{0, 1\}^{\eta}$, as follows:

$$|\chi,\ 0_{\eta q}\rangle \rightarrow |0_{\eta}, C(\chi)\rangle, \tag{12}$$

where, for $a > 0$, 0_a represents a string of a zeroes, and

$$C(\chi) = \sum_{\xi \in \{0,1\}^{\eta}, \xi \prec \chi} \Lambda\left(\xi; \lambda_0^{\diamond}, \lambda_1^{\diamond}\right), \tag{13}$$

where $\Lambda\left(\xi; \lambda_0^{\diamond}, \lambda_1^{\diamond}\right)$ is obtained from Eq. (4) and $\prec$ denotes some total order on the strings in $\{0, 1\}^n$. The invention will specify a computationally simple-to-implement lexicographical order below. Observe that for every eigenstate $|\chi\rangle$, $C(\chi)$ is a number in the real interval (0, 1). Hence, given $C(\chi)$, the invention writes $|C(\chi)\rangle$ using the terminology of Section 2.5. Intuitively, $C(\chi)$ is the sum of the eigenvalues of all eigenstates of length n that are less than or equal

to the χ in the total order $\prec$. Since C*(X)* is a monotonically increasing function of the eigenstates arranged in lexicographical order, it is uniquely decodable. In other words, the transformation

$$|0_\eta, C(\chi)\rangle \rightarrow |\chi, 0_{\eta q}\rangle, \tag{14}$$

exists for every eigenstate $|\chi\rangle, \chi \in \{0, 1\}^\eta$. Hence, Eq. (12) is reversible, and can be implemented as an unitary transformation.

Each eigenvalue in the sum Eq. (13) is a product of *n* numbers each of which has a precision of *q* bits. Hence, each eigenvalue can be written as a fractional binary number with at most *nq* nonzero significant bits. Finally, this implies that, for each eigenstate, the number C(χ) has precision no more than *nq* bits. In other words, the encoder is a unitary transformation from $H_2^{\otimes \eta}$ to a 2^n-dimensional subspace of $H_2^{\otimes \eta q}$. However, since generally $q > 1$, this hardly constitutes data compression. The invention now achieves compression by truncating a large number of nonsignificant bits of C(χ).

For a given truncation parameter $k \geq 0$ and a given eigenstate $|\chi\rangle, \chi \in \{0,1\}^\eta$ the invention defines the truncated encoder transform as

$$\left|\chi, 0_{\eta q}\right\rangle \rightarrow \left|0_{\eta}, C(\chi)_{[k]} 1_{\eta q-k}\right\rangle, \qquad \text{Eq. (15)}$$

where $C(\chi)_{[k]}$ denotes the truncation of $C(\chi)$ to the k most significant qubits. Observe that only the first k qubits on the right-hand side depend upon the eigenstates, and, hence, only these bits need be transmitted. All the information present in the eigenstate χ has been captured into $C(\chi)$ in a reversible fashion. Hence, compression does not cause any loss of information.

Consequently, the encoder in Eq. (15) maps messages of a fixed-length n to codewords of fixed-length k. In other words, the encoder is a unitary transformation from $H_2^{\otimes \eta}$ to a subspace of $H_2^{\otimes k}$.

The decodability of the untruncated map in Eq. (12) is immediate from the fact that $C(\chi)$ is a monotonically increasing function of the eigenstates arranged in the lexicographical order. In contrast, the decodability of the truncated map in Eq. (15) is a delicate matter. If $k < n$, then the truncated map cannot hope to correctly decode all the eigenstates. However, fortunately, the invention only needs to correctly decode the good eigenstates. The invention can discard the bad eigenstates, since we have assumed that the event $\left(\left\{\left|I_{\tau}\right\rangle \stackrel{m}{=} \left|0\right\rangle\right\}\right)$ has occurred, and in this case, bad eigenstates have already been discarded. So, there was no need to either encode or decode the bad eigenstates.

The invention now establishes that if the threshold parameter τ and truncation parameter k are carefully selected, then inverse of Eq. (15) exists for all the good eigenstates.

If,

$$\tau = \left\lceil \eta\left(\lambda_1 + \frac{\delta}{\log \lambda_0 / \lambda_1}\right)\right\rceil, \tag{16}$$

$$\mathrm{k} \geq \eta \mathrm{S}(\rho) + \eta \mathrm{D}\left(\lambda_0 \middle\| \lambda_0^{\diamond}\right) + \eta\delta + \log(\lambda_0 / \lambda_1). \tag{17}$$

Then, there exists a decoder such that, for every X in G^{τ},

$$\left|0_{\eta}, \mathrm{C}(\chi)_{[\mathrm{k}]} 1_{\eta \mathrm{q}-\mathrm{k}}\right\rangle \rightarrow \left|\chi, 0_{\eta \mathrm{q}}\right\rangle. \tag{18}$$

This is shown in the following. Given the encoding $\left|\mathrm{C}(\chi)_{[\mathrm{k}]} 1_{\eta \mathrm{q}-\mathrm{k}}\right\rangle$ of the eigenstate $\left|\chi\right\rangle$, the invention defines the corresponding decoded or reconstructed eigenstate as $\left|\tilde{\chi}\right\rangle, \tilde{\chi} \in \{0,1\}^{\eta}$, that satisfies the following two inequalities:

$$\mathrm{C}(\tilde{\chi}) \leq \mathrm{C}(\chi)_{[\mathrm{k}]} + \sum_{\mathrm{i}=\mathrm{k}+1}^{\eta \mathrm{q}} 2^{-\mathrm{i}} \qquad \text{Eq. (19)}$$

$$\mathrm{C}(\chi)_{[\mathrm{k}]} + \sum_{\mathrm{i}=\mathrm{k}+1}^{\eta \mathrm{q}} 2^{-\mathrm{i}} < \mathrm{C}(\tilde{\chi}) + \Lambda\left(\tilde{\chi}; \lambda_0^{\diamond}, \lambda_1^{\diamond}\right). \qquad \text{Eq. (20)}$$

In general, owing to truncation, the decoded eigenstate $\tilde{\chi}$ need not equal the original eigenstate X. The invention now shows that for values of τ as in Eq. (16), for values of k as in Eq. (17), and for all good eigenstates, the inequalities Eq. (19) and Eq. (20) are satisfied if and only if $\tilde{\chi} = \chi$. Suppose that $\tilde{\chi} = \chi$. In this case, the first inequality Eq. (19) is trivial, and holds for all X in $\{0,1\}^n$. Now, observe that the second inequality Eq. (20) holds if

$$\Lambda\left(\tilde{\chi};\lambda_0^{\diamond},\lambda_1^{\diamond}\right) = \Lambda\left(\chi;\lambda_0^{\diamond},\lambda_1^{\diamond}\right) \geq 2^{-k} > \sum_{i=k+1}^{\eta q} 2^{-i}.$$

It follows from Eq. (4) that the second inequality Eq. (20) holds if

$$\left(\lambda_1^{\diamond}\right)^{w(\chi)}\left(\lambda_0^{\diamond}\right)^{\eta-w(\chi)} \geq 2^{-k}.$$

The invention would like the above inequality to hold for all good eigenstates. Since $\left(\lambda_1^{\diamond}\right)^{\theta}\left(\lambda_0^{\diamond}\right)^{\eta-\theta}, 0 \leq \theta \leq \eta,$ is a decreasing function of θ, it is sufficient that the above inequality holds for the good eigenstates corresponding to the smallest good eigenvalue. If the invention selects τ as in Eq. (16), then the smallest eigenvalue is larger than $\left(\lambda_1^{\diamond}\right)^{\tau}\left(\lambda_0^{\diamond}\right)^{\eta-\tau}$.

Hence, the invention requires that $\left(\lambda_1^{\diamond}\right)^{\tau}\left(\lambda_0^{\diamond}\right)^{\eta-\tau} \geq 2^{-k}$.

Equivalently, the invention requires that $(\lambda_1)^{\tau}(\lambda_0)^{\eta-\tau}\left(\frac{\lambda_1^{\diamond}}{\lambda_1}\right)^{\tau}\left(\frac{\lambda_0^{\diamond}}{\lambda_0}\right)^{\eta-\tau} \geq 2^{-k}$.

It follows from simple algebraic manipulations that the above holds if

$$k \geq \eta S(\rho) + \eta D\left(\lambda_0 \middle\| \lambda_0^{\diamond}\right) + \eta\delta + \log(\lambda_0 / \lambda_1).$$

This is exactly the requirement in Eq. (17).

The invention now establishes the converse, that is, if $\chi \neq \tilde{\chi}$, then both Eq. (19) and Eq. (20) do not hold. There are two cases: either $\chi \prec \tilde{\chi}$ or $\tilde{\chi} \prec \chi$. In the former case, Eq. (19) cannot hold and in the latter case Eq. (20) cannot hold.

Observe that the desired encoder transform in Eq. (15) annihilates the quantum state *X*. This is necessary since both $|\chi\rangle$ and $|C(\chi)_{[k]}\rangle$ contain the same information, and since quantum states cannot be cloned, it is impossible to faithfully transmit weighted superpositions of different $|\chi\rangle$ without the sender

obliterating her knowledge about it in the process of transforming the state into a weighted superposition of $\left|C(\chi)_{[k]}\right\rangle$.

Observe that the untruncated map in Eq. (12) and the truncated map in Eq. (15) map one eigenstate to one encoded state. Hence, they can be thought of as unitary transforms that are permutations of the basis states.

So far, the invention has specified the desired encoder Eq. (15) and the corresponding decoder in Eq. (18) in terms of the eigenstates alone. For the sake of completeness, by using linearity of the encoder and the decoder, the invention now describes their action on the quantum message of interest:

$$\left|\hat{\psi}_{[\eta]},0_{\eta q}\right\rangle = \sum_{\chi\in G\tau}\langle\chi\left|\hat{\psi}_{[\eta]}\right\rangle\left|\chi,0_{\eta q}\right\rangle$$

$$\xrightarrow{\text{encode}} \sum_{\chi\in G\tau}\langle\chi\left|\hat{\psi}_{[\eta]}\right\rangle\left|0_{\eta},C(\chi)_{[k]}1_{\eta q-k}\right\rangle$$

$$\xrightarrow{\text{transmit}} \sum_{\chi\in G\tau}\langle\chi\left|\hat{\psi}_{[\eta]}\right\rangle\left|C(\chi)_{[k]}\right\rangle$$

$$\xrightarrow{\text{prepare}} \sum_{\chi\in G\tau}\langle\chi\left|\hat{\psi}_{[\eta]}\right\rangle\left|0_{\eta},C(\chi)_{[k]}1_{\eta q-k}\right\rangle$$

$$\xrightarrow{\text{decode}} \sum_{\chi\in G\tau}\left\langle\chi\left|\hat{\psi}_{[\eta]}\right\rangle\right|\chi,0_{\eta q}\rangle$$

$$= \left|\hat{\psi}_{[\eta]},0_{\eta q}\right\rangle,$$

where the invention has implicitly used the fact that a measurement on the qubit $|I_\tau\rangle$ has been made, and the event $\left\{|I_\tau\rangle \stackrel{m}{=} |0\rangle\right\}$ has occurred. The foregoing series of equations capture the essence of the invention. The eigenstates are encoded, transmitted, and decoded without any loss of information. Conceptually, encoding and decoding are reversible operations that are conceptual inverses of each other, hence, no information is lost in the entire process.

The invention now proposes quantum algorithms and associated quantum circuits to efficiently realize the encoder in Eq. (15) and the corresponding decoder in Eq. (18).

First, the invention considers the computation of the function $C(\chi)$ in Eq. (13). A straightforward algorithm for computing $C(\chi)$ by explicitly performing the summation would require an exponential amount of complexity in the block size *n*. One of the main contributions of classical arithmetic coding is to observe that if the invention selects the total order $\prec$ in Eq. (13) to be the following lexicographical order, then the function $C(\chi)$ can be efficiently computed. If $\xi \equiv \xi_1 \xi_2 \cdots \xi_\eta$, and $\chi \equiv \chi_1 \chi_2 \cdots \chi_\eta$ are in $\{0,1\}^n$ then the invention says that

$\xi \prec \chi$ if and only if $\sum_{i=1}^{\eta} \xi_i 2^{i-1} < \sum_{i=1}^{\eta} \chi_i 2^{i-1}$.

Under this definition of the total order $\prec$ the invention can write the function $C(\chi)$ recursively as follows, see, [J. Rissanen et al., *supra*, (1)]:

$$C(\chi) = 0$$

for i=1 to n do

if ($Xi = 0$)

$$C(X) = C(X) \times \lambda_0^{\diamond}$$

else

$$C(\chi) = C(\chi) \times \lambda_1^{\diamond} + \lambda_0^{\diamond}$$

endif

endfor

Instead of the lexicographical order in Eq. (21), the invention can also use the following dual order. If $\xi \equiv \xi_1\xi_2\cdots\xi_\eta$ and $\chi \equiv \chi_1\chi_2\cdots\chi_\eta$ are in $\{0, 1\}^n$, then the invention says that

$$\xi \overset{\text{dual}}{\prec} \chi \text{ if and only if } \sum_{i=1}^{\eta} \xi_i 2^{-i+1} < \sum_{i=1}^{\eta} \chi_i 2^{-i+1}.$$

Under this dual definition, the invention can also write the function $C(\chi)$ recursively, see, (Rissanen et al., *supra*, (2)). Although both the recursions are amenable to a quantum implementation, the recursion corresponding to the total order in Eq. (21) turns out to slightly simpler and, hence, is used in this disclosure.

Important parts of the encoding and decoding algorithms are multiplication and division, respectively, and in order to build the quantum coders, the invention must first construct quantum algorithms for such arithmetic. Suitable addition and subtraction circuits have already been described in the

literature (D. Beckman, A.N. Chari, S. Devabhaktuni, and J. Preskill, "Efficient networks for quantum factoring," *Physical Review* A, vol. 54, no. 2, pp. 1034-1063, 1996, http://xxx.lanl.gov/abs/quant-ph/9602016, and R. Cleve and D.P. DiVincenzo, "Schumacher's quantum data compression as a quantum computation," *Physical Review A*, vol. 54, pp. 2636-2650, October 1996, each incorporated herein by reference), but appropriate multiplication and division algorithms have not been. These are described below.

The invention presents in Figure 4 an algorithm to multiply $\left(|A\rangle, |B\rangle, |R\rangle, i\right)$ that takes the following inputs: (a) a fixed index i, $i = 1, 2, \cdots, n$, (b) nq qubit register $|A\rangle$ such that all but the first $(i\text{-}1)$ q qubits are zeroes, (c) q qubit register $|B\rangle$, and (d) q qubit register $|R\rangle$. The algorithm also requires a nq qubit temporary register $|T\rangle$ that is initialized and finalized to $|0_{nq}\rangle$. The algorithm computes $|A, R\rangle \rightarrow |AB + 2^{-(i-1)q-1}R, 0_q\rangle$, where multiplications and additions are to be interpreted by treating A, B, and R as fractional binary numbers. A quantum circuit which implements the algorithm is shown in Figure 5. The steps in Figure 4 correspond simply to a quantum version of the classical algorithm for multiplying two numbers A and B where there is an additional quantity that is added at the end.

The invention terms the conjugate inverse of this algorithm as divide $\left(|A\rangle, |B\rangle, |R\rangle, i\right)$. Given a nq qubit register $|A\rangle$ such that all but the first iq

qubits are zeroes, a q qubit register $|B\rangle$, and a q qubit register $|R\rangle$ that is initialized to $|0_q\rangle$, the circuit divide $\left(|A\rangle,|B\rangle,|R\rangle,i\right)$ uses a nq qubit temporary register $|T\rangle$ that is initialized and finalized to $|0_{\eta q}\rangle$ and divides A by B up to the first $(i-1)q$ bits, and stores the quotient also in A, and keeps the q qubit remainder in R.

The invention now uses the ideas from arithmetic recursions, and the above circuits for multiplication and division to construct building blocks for the desired encoder in Eq. (15). In Figure 6, the invention presents two recursive algorithms "E" and "D." Formally and literally, these algorithms are inverses of each other: lines E2-E8 are literal inverses of lines D7-D13, lines E9-E13 are literal inverses of lines D2-D6, and, finally, the for loop in the algorithm E processes the message symbols in the original order from 1 to n while the for loop in the algorithm D emits the message symbols in the inverse order from n to 1. The invention exhibits quantum circuits for implementing the algorithms E and D in Figures 7 and 8, respectively. Observe that these circuits are also quantum-mechanical inverses of each other.

The invention intends to use the algorithms E and D with two different sets of inputs. The invention now explains the functionality of these algorithms on the first set of inputs.

Let $|\chi\rangle, \chi \in \{0,1\}^{\eta}$, denote any eigenstate. The algorithms *D* and *E*, respectively, compute the following maps:

$$D_1: |0_\eta, C(\chi), 0_{\eta q}\rangle \rightarrow |\chi, 0_{\eta q}, 0_{\eta q}\rangle, \qquad \text{Eq. (23)}$$

$$E_1: |\chi, 0_{\eta q}, 0_{\eta q}\rangle \rightarrow |0_\eta, C(\chi), 0_{\eta q}\rangle \qquad \text{Eq. (24)}$$

With the inputs as above, E_1 is a quantum version of the arithmetic recursion presented above. The desired assertion for D_1 follows by observing that it is a literal inverse of E_1. In both of these cases, the quantum register $|R_1 R_2 \cdots R_\eta\rangle$ always remains in the same initial state $|0_{\eta q}\rangle$.

This furnishes a way of implementing Eq. (12) and its inverse Eq. (14). Recall, however, that to achieve compression the invention is interested in implementing Eq. (15). The obvious strategy of first implementing Eq. (12) and simply transmitting the *k* most significant qubits of $|C(\chi)\rangle$ does not work, since these *k* qubits are entangled with the *nq-k* least significant qubits of $|C(\chi)\rangle$. Hence, a measurement on these *nq-k* least significant qubits will irreversibly change the *k* most significant qubits. To avoid such an accident, the invention must erase the *nq-k* qubits. This is the central difficulty that the invention must overcome. The invention now explains the functionality of the algorithms *E* and *D* on the second set of inputs.

Suppose that a measurement on the qubit $|I_\tau\rangle$ has been made, and the event $\{|I_\tau\rangle \stackrel{m}{=} |0\rangle\}$ has occurred. Let $|\chi\rangle, \chi \in G_\tau$, denote any good eigenstate. The algorithms *D* and *E*, respectively, compute the following maps:

$$D_2: |0_\eta,\ C(\chi)_{[k]} 1_{\eta q-k},\ 0_{\eta q}\rangle \longrightarrow |\chi,\ 0_{\eta q}, R_1 R_2 \cdots R_\eta\rangle \quad (25)$$

$$E_2: |\chi,\ 0_{\eta q},\ R_1 R_2 \cdots R_\eta\rangle \longrightarrow |0_\eta,\ C(\chi)_{[k]} 1_{\eta q-k},\ 0_\eta q\rangle. \quad (26)$$

The invention establishes the assertion for D_2 in detail. The desired assertion for E_2 follows by observing that it is a literal inverse of D_2. Fix a good eigenstate $|\chi\rangle = |\chi_1 \chi_2 \cdots \chi_\eta\rangle$. As shown above, $|\chi\rangle$ can be decoded correctly; the gist of what follows is that not only may $|\chi\rangle$ be decoded correctly, in fact, it may be decoded correctly in a sequential or recursive fashion. For a index *i*, i=1, 2, $\cdots, \eta$, recall that $|\chi_{[i]}\rangle \equiv |\chi_1 \chi_2 \cdots \chi_i\rangle$.

The invention first shows that lines D7-D13 in Figure 6 behave as desired. For any i =1, 2, $\cdots, \eta$ and for real number C, observe that if

$$C(\chi_{[i]}) \le C < C(\chi_{[i]}) + \Lambda\left(\chi_{[i]}; \lambda^{\diamond}_0, \lambda^{\diamond}_1\right) \quad (27)$$

then, after the computation in lines D7-D13, the invention has

$$C(\chi_{[i-1]}) \le C < C(\chi_{[i-1]}) + \Lambda(\chi_{[i-1]}; \lambda_0^{\diamond}, \lambda_1^{\diamond})$$

However, the invention has from Eq. (19) and Eq. (20) that, if the invention sets $C = C(\chi)_{[k]} + \sum_{i=k+1}^{\eta q} 2^{-i}$, then the inequality Eq. (27) holds for $i = n$. Hence, by induction, the inequality Eq. (27) holds for all $i=1, 2, \cdots, \eta$.

Step 2: The invention now shows that lines D2-D6 behave as desired. For any $i=1, 2, \cdots, \eta$ and for real number C, if the inequality Eq. (27) holds, then

$$C \ge \lambda_0^{\diamond} \text{ if and only if } C(\chi_{[i]}) \ge \lambda_0^{\diamond} \qquad (28)$$

The "if" part of Eq. (28) follows trivially from Eq. (27). To see the "only if" part, observe that if $C \ge \lambda_0^{\diamond}$, then, by Eq. (27), $C(\chi_{[i]}) + \Lambda(\chi_{[i]}; \lambda_0^{\diamond}, \lambda_1^{\diamond}) > \lambda_0^{\diamond}$.

Hence, $C(\chi_{[i]}) > \lambda_0^{\diamond} - \Lambda(\chi_{[i]}; \lambda_0^{\diamond}, \lambda_1^{\diamond})$.

Hence, again by Eq. (27),

$$C \ge C(\chi_{[i]}) > \lambda_0^{\diamond} - \Lambda(\chi_{[i]}; \lambda_0^{\diamond}, \lambda_1^{\diamond}).$$

The only allowed values of $C(\chi_{[i]})$ that satisfy the above inequality are $C(\chi_{[i]}) \ge \lambda_0^{\diamond}$ as desired.

Observe that Eq. (25) is almost the desired decoder Eq. (18) except for the "remainder" $|R_1R_2\cdots R_\eta\rangle$, which is left over. Once again, the decoded state $|\chi\rangle$ is entangled with this remainder, and, hence, the remainder must be erased. Similarly, Eq. (26) is almost the desired encoder Eq. (15) except that it requires the above left over remainder as an input.

It follows from the above discussion that the algorithms described above do not, in themselves, yield either the desired encoder Eq. (15) or the decoder Eq. (18). The invention now presents an algorithm, in Figure 9, the desired encoder. The desired decoder is obtained by literally running the encoder in reverse.

The circuit in Figure 9 is started by applying the transformation E_1

$$E_1:|\chi,0_{\eta q},0_{\eta q}\rangle \rightarrow |0_\eta, C(\chi),0_{\eta q}\rangle.$$

After the *k* most significant qubits of $|C_{(\chi)}\rangle$ are copied (of course, they are not truly copied in the classical sense, since qubits cannot be cloned; they are entangled with an auxiliary set of qubits prepared in the $|0\rangle$ state), the output of E_1 is acted upon by the transformation D_1

$$D_1:|0_\eta, C(\chi),0_{\eta q}\rangle \rightarrow |\chi,0_{\eta q},0_{\eta q}\rangle.$$

This has the effect of annihilating all the *nq* qubits of $|C(\chi)\rangle$. However, it recreates the input quantum state $|\chi\rangle$ which must also be erased. Now, by employing the *k* copied qubits $|C(\chi)_{[k]}\rangle$, the invention can apply D_2

$$D_2:\left|0_\eta, C(\chi)_{[k]} 1_{\eta q-k}, 0_{\eta q}\right\rangle \rightarrow \left|\chi, 0_{\eta q}, R_1 R_2 \cdots R_\eta\right\rangle.$$

The quantum state $\left|\chi\right\rangle$ produced at the output of D_2 is used to erase the same quantum state produced at the output of D_1. Now, by applying E_2 to the output produced by D_2, the invention has the desired output:

$$E_2:\left|\chi, 0_{\eta q}, R_1 R_2 \cdots R_\eta\right\rangle \rightarrow \left|0_\eta, C(\chi)_{[k]} 1_{\eta q-k}, 0_{\eta q}\right\rangle.$$

In the end, the invention is guaranteed that no quantum register in Figure 9 is entangled with the final output $\left|C(\chi)_{[k]}\right\rangle$. Hence, the output can now be freely transmitted. Observe that the cascade of E_1 and D_1 is the identity map, and, similarly, the cascade of D_2 and E_2 is also the identity map.

The invention now analyzes the complexity of implementing the E_1 block in Figure 9. The E_1 block can be implemented using the circuit presented in Figure 7. The "$\geq$" operator compares a *nq* qubit register C to a *q* bit constant. Using the TEST-GREATER-THAN circuits [R. Cleve et al., *supra*], such comparisons can be implemented quantum-mechanically in O(*nq*) elementary quantum gates. The invention has used a "swap" or $\leftrightarrow$ operator in circuits for multiply and divide. A quantum-mechanical operator that swaps two quantum registers of length *q* can be implemented using O(*q*) quantum Fredkin gates (E. Fredkin and T. Toffoli, "Conservative logic," *International Journal of Theoretical Physics,* vol. 21, no.

3/4, pp. 219-253, 1982, and H.F. Chau and F. Wilczek, "Simple realization of the Fredkin gate using a series of two-body operators," *Physical Review Letters*, vol. 75, no. 4, pp. 748-750, 1995, each incorporated herein by reference). For the index i, $1 \leq i \leq n$, the overall circuit for M_i can be implemented in $O(i^2q^2)$ elementary quantum gates. In conclusion, the overall circuit for the E_1 block can be implemented using $O(n^3q^2)$ elementary quantum gates. The blocks D_1, E_2, and D_2 have the same complexity as the block E_1. Hence, the overall encoder in Figure 9 can also be implemented using $O(n^3q^2)$ elementary quantum gates. Also, using similar reasoning, it follows that the overall encoder in Figure 9 has a $O(n^3q^2)$ computational complexity.

While the overall methodology of the invention is described above, the invention can be embodied in any number of different types of systems and executed in any number of different ways, as would be known by one ordinarily skilled in the art. For example, as illustrated in Figure 10, a typical hardware configuration of an information handling/computer system in accordance with the invention preferably has at least one processor or central processing unit (CPU) 1000. For example, the central processing unit 1000 could include various image/texture processing units, mapping units, weighting units, classification units, clustering units, filters, adders, subtractors, comparators, etc. Alternatively, as would be known by one ordinarily skilled in the art given this disclosure, multiple specialized CPU's (or other similar individual functional units) could perform the same processing, mapping, weighting, classifying, clustering, filtering, adding, subtracting, comparing, etc.

The CPU 1000 is interconnected via a system bus 1001 to a random access memory (RAM) 1002, read-only memory (ROM) 1003, input/output (I/O) adapter 1004 (for connecting peripheral devices such as disk units 1005 and tape drives 1006 to the bus 1001), communication adapter 1007 (for connecting an information handling system to a data processing network) user interface adapter 1008 (for connecting peripherals 1009-1010 such as a keyboard, mouse, imager, microphone, speaker and/or other interface device to the bus 1001), a printer 1011, and display adapter 1012 (for connecting the bus 1001 to a display device 1013). The invention could be implemented using the structure shown in Figure 10 by including the inventive method, described above, within a computer program stored on the storage device 1005.

The invention has constructed a quantum algorithm for block compression of quantum information which is an analog of classical arithmetic coding. In contrast to the classical case, the quantum algorithm must take extra care to leave behind no residual traces of its past history. The algorithm thus begins by projecting the state into the typical subspace, then a sequence of encoding and decoding using finite precision arithmetic is done in a manner so as to obliterate all possible imprecisions.

Unlike the classical algorithms for arithmetic coding, the multiplication steps used in the invention's algorithm require a linearly increasing precision in the block size n. In the classical case, it is known how to implement these multiplications using precision that is independent of n [J. Rissanen et al., *supra*].

It is straightforward to perform this algorithm in parallel, so as to reduce the number of time-steps necessary for its circuit implementation. Multiplication and addition are known to be in $NC(1)$, and believed to also be in the quantum counterpart to this class, so that it is possible to obtain an $O(n)$ running time implementation of the inventions algorithm. Quantum circuits such as the one the invention presented may also find use as reversible classical circuits, which potentially require much less power for their execution when using technologies such as reversible CMOS or charge recovery logic see, (S. Younis and T. Knight, "Non dissipative rail drivers for adiabatic circuits," in *Proceedings of the Sixteenth Conference on Advanced Research in VLSI* 1995 (Los Alamitos, CA), pp. 404-414, IEEE Comput. Soc. Press, 1995), incorporated herein by reference). Finally, the invention has considered block arithmetic codes.

While the invention has been described in terms of preferred embodiments, those skilled in the art will recognize that the invention can be practiced with modification within the spirit and scope of the appended claims.